

D8.1 LEGAL COMPLIANCE FOR NON-EU COUNTRIES

Lead Author: Hande İrem SADI

With contributions from: Magdalena Kogut Czarkowska, Eleni Moraiti (TLX), Alicia Jimenez (GRAD)

Reviewer: Magdalena Kogut Czarkowska, Eleni Moraiti (TLX), Alicia Jimenez (GRAD)

Deliverable nature	Report (R)
Dissemination level	Public (PU)
Delivery date	30-11-2024
Version	2.2
Total number of pages	20
Keywords	TRUMPET, Federated Learning, Healthcare Data Integration, Privacy, GDPR Compliance, Non-EU Countries, Digital Health

EXECUTIVE SUMMARY

This deliverable addresses the essential alignment of data protection standards between Türkiye's KVKK (Data Protection Law) and the EU's GDPR in the context of the TRUMPET platform —a Federated Learning (FL) secured platform for healthcare solutions within the Horizon Civil Security for Society program. This alignment aims to establish a consistent and comprehensive approach to data processing and privacy compliance, ensuring regulatory harmony between national and international standards.

The deliverable conducts a detailed comparison of KVKK and GDPR, assessing specific legal requirements that impact data handling, privacy protocols, and ethical governance. Given Türkiye's unique regulatory landscape, the objective is to bridge gaps where KVKK and GDPR diverge, ensuring that TRUMPET's platform integration and pilot activities remain legally compliant and ethically responsible.

Through this alignment, the deliverable also provides a structured approach to supporting the platform's pilot projects across a broader geographical scope, enhancing the artificial intelligence model's learning process with more data and ensuring the privacy of participants. By closely monitoring and adjusting data practices to meet KVKK's standards, this work creates a foundational framework that can guide similar non-EU integrations, contributing to ethically sound and legally consistent data exchanges across diverse jurisdictions.

Ultimately, this deliverable serves as a reference model for deploying federated learning healthcare solutions like TRUMPET in non-EU countries, like Türkiye, bolstering data security, transparency, and legal compliance while advancing the adaptability of training healthcare AI algorithms in a secure manner through FL platforms approach on a global scale.

DOCUMENT INFORMATION

Grant agreement No.	101070038	Acronym	TRUMPET
Full title	TRUstworthy Multi-site Privacy Enhancing Technologies		
Call	HORIZON-CL3-2021-CS-01-04		
Project URL	https://cordis.europa.eu/project/id/101070038		
EU project officer	Ioannis ASKOXYLAKIS		

Deliverable	Number	D8.1	Title	Legal compliance for non-EU countries
Work package	Number	WP8	Title	TRUMPET Validation for Widening Activity
Task	Number	T8.1	Title	Completing Legal Checks

Date of delivery	Contractual	Mxx	Actual	Mxx
Status	version 2.2	<input checked="" type="checkbox"/> Final version		
Nature	<input checked="" type="checkbox"/> R <input type="checkbox"/> DEM <input type="checkbox"/> DMP <input type="checkbox"/> DEC <input type="checkbox"/> ETHICS <input type="checkbox"/> OTHER			
Dissemination level	<input checked="" type="checkbox"/> Public <input type="checkbox"/> Sensitive			

Authors (partners)	MOH
Responsible author	Hande İrem SADI hiremsadi@saglik.gov.tr

Summary (for dissemination)	This deliverable will conduct a comparison of Turkish GDPR and EU GDPR and other regulations within the scope of the platform integration and the pilots' execution. This alignment seeks to make data protection and privacy standards consistent at the national and international levels, ensuring that data processing processes are managed more consistently and appropriately.
Keywords	<i>TRUMPET, Federated Learning, Healthcare Data Integration, Privacy, GDPR Compliance, Non-EU Countries, Digital Health</i>

VERSION LONG			
Issue Date	Rev. No.	Author	Change
28/11/2024	1.0	Hande İrem SADİ (MOH)	First Draft
02/12/2024	1.1	Magdalena Kogut (TLX), Eleni Moraiti (TLX)	Document Review
05/12/2024	1.2	Alicia Jiménez (GRAD)	Document Review
12/12/2024	2.0	Hande İrem SADİ (MOH)	Second Draft
17/12/2024	2.1	Magdalena Kogut (TLX), Eleni Moraiti (TLX)	Document Review
18/12/2024	2.2	Hande İrem SADİ (MOH)	Final Version

TABLE OF CONTENTS

<u>TRUStworthy Multi-site Privacy Enhancing Technologies</u>	<u>1</u>
<u>Executive summary.....</u>	<u>2</u>
<u>Document information</u>	<u>3</u>
<u>Table of contents</u>	<u>5</u>
<u>Abbreviations and Acronyms.....</u>	<u>6</u>
<u>1 Introduction.....</u>	<u>7</u>
<u>2 GDPR and KVKK: A Comparative Analysis for TRUMPET Integration</u>	<u>9</u>
<u>3 Regulatory Challenges in Bridging GDPR and KVKK</u>	<u>14</u>
<u>4 Integration Process for the TRUMPET Platform in Türkiye as a Non-EU Country.....</u>	<u>16</u>
<u>4.1 Technical Modifications for Local Compliance.....</u>	<u>16</u>
<u>4.2 Testing and Validation.....</u>	<u>17</u>
<u>4.3 Broader Implications for Türkiye’s Healthcare System.....</u>	<u>17</u>
<u>5. Conclusion.....</u>	<u>19</u>
<u>References</u>	<u>20</u>

DE



TRUStworthy Multi-site Privacy Enhancing Technologies

ABBREVIATIONS AND ACRONYMS

DPA - Data Protection Authority

EU - European Union

FL- Federated Learning

GDPR - General Data Protection Regulation

KVKK - Kişisel Verilerin Korunması Kanunu (Turkish Data Protection Law)

SCCs- Standard Contractual Clauses

TRUMPET - TRUStworthy Multi-site Privacy Enhancing Technologies



Funded by
the European Union

Trumpet project has received funding from a Research and Innovation action activity under Horizon Europe Framework Programme with Grant Agreement No.101070038

1. Introduction

The TRUMPET project, an integral part of the Horizon Civil Security for Society program, aims to establish an advanced Federated Learning (FL) platform tailored for healthcare research. The platform's core objective is to empower researchers to collaboratively develop models and tools while ensuring patient data privacy and security. As a decentralized and privacy-preserving technology, federated learning facilitates the creation of robust healthcare solutions without compromising sensitive data. For European Union (EU) users, the project aligns with the General Data Protection Regulation (GDPR), while for Türkiye, significant adaptations are required to comply with the Turkish Data Protection Law (KVKK).

The primary regulatory challenge faced in the implementation of TRUMPET is reconciling the stringent requirements of GDPR with those of Türkiye's KVKK. GDPR, which governs data protection within the EU, emphasizes principles such as consent, data minimization, purpose limitation, and accountability. In comparison, Türkiye's KVKK shares similar objectives but includes specific clauses that address unique concerns, especially in regard to data transfer, processing permissions, and the clarity of consent mechanisms. Additionally, KVKK's focus on protecting locally processed data introduces a need for tailored solutions that address Türkiye's regulatory nuances without disrupting TRUMPET's interoperability with GDPR-compliant frameworks.

Actually, the primary regulatory challenge in implementing TRUMPET arises from the need to reconcile the stringent requirements of the EU's General Data Protection Regulation (GDPR) with Türkiye's Personal Data Protection Law (KVKK, Law No. 6698). Both frameworks share overarching objectives, such as safeguarding personal data, ensuring transparency, and protecting individual rights. However, there are critical differences in the interpretation and implementation of these principles, particularly concerning data processing, consent mechanisms, and cross-border data transfers.

GDPR emphasizes principles such as consent, data minimization, purpose limitation, and accountability. Under GDPR, consent must be freely given, specific, informed, and unambiguous, as stated in Article 4(11) and further elaborated in Recital 32. KVKK also upholds the importance of explicit consent under Article 3, ensuring it is informed and freely given. However, KVKK additionally stresses culturally and legally contextualized requirements, which can lead to differences in how consent is implemented and enforced.

Regarding data processing, GDPR permits processing based on multiple lawful grounds, including performance of a contract, compliance with a legal obligation, and legitimate interests, as outlined in Article 6. KVKK aligns with these principles but adds further specificity in Article 5, listing conditions such as explicit consent, legal obligations, and the necessity for contract fulfilment. Notably, KVKK explicitly requires organizations to inform data subjects about data usage purposes and legal grounds before processing.

A significant distinction arises in data transfer regulations. GDPR allows data transfer outside the EU to countries ensuring "adequate protection," as stated in Articles 44–46, or under specific mechanisms like Standard Contractual Clauses (SCCs). KVKK's Article 9 introduces a stricter approach for international data transfers. It requires either explicit consent from data subjects or the

presence of “adequate safeguards” approved by the Personal Data Protection Board, making cross-border compliance more intricate for projects like TRUMPET.

These nuanced and localized requirements introduce complexities for projects aiming to harmonize operations across jurisdictions. Tailored solutions are essential to address Türkiye’s unique regulatory concerns without undermining the project’s interoperability with GDPR-compliant frameworks. Section 2 of this deliverable provides a detailed breakdown of KVKK’s key provisions, such as the conditions for data processing, rules for cross-border data transfers, and consent requirements, and compares them with GDPR standards to outline practical solutions for TRUMPET.

Federated learning, as the backbone of TRUMPET, inherently aligns with many of these regulatory requirements by enabling data to remain localized while allowing the aggregation of knowledge across distributed systems. This approach not only reduces the risk of data breaches but also provides a practical foundation for compliance with both GDPR and KVKK. However, achieving full compliance requires the integration of jurisdiction-specific mechanisms, such as dynamic consent processes and localized incident response plans, into the platform’s operational design. These additions ensure that TRUMPET can adapt to varying legal contexts while maintaining its primary focus on privacy and innovation.

One of the key tasks in this project is addressing these regulatory differences in order to enable federated learning while ensuring compliance with both GDPR and KVKK. This requires in-depth analysis of data protection principles in both jurisdictions and the development of a comprehensive strategy for integrating these requirements into TRUMPET’s platform. As a result, the platform can serve as a model for how digital health technologies can navigate complex regulatory landscapes, fostering greater trust among stakeholders and promoting collaboration across borders.

This deliverable outline how TRUMPET’s implementation within Türkiye will bridge these regulatory frameworks, ensuring compliance with local ethical, legal, and data-handling standards. By focusing on both GDPR and KVKK compatibility, the project emphasizes the importance of secure data management and the protection of personal health information. Moreover, it highlights the potential for federated learning to address broader challenges in healthcare data sharing, setting a precedent for future initiatives seeking to balance innovation with privacy. The following sections delve deeper into the TRUMPET platform’s core objectives and Türkiye’s distinct regulatory environment.

2. GDPR and KVKK: A Comparative Analysis for TRUMPET Integration

The TRUMPET project operates at the intersection of two critical regulatory frameworks: The General Data Protection Regulation (GDPR) of the European Union and Türkiye's Personal Data Protection Law (KVKK). These frameworks share the fundamental goal of safeguarding personal data, particularly in sensitive areas such as healthcare. However, their nuanced differences in scope, mechanisms, and implementation present unique challenges for integrating a federated learning platform like TRUMPET, which aims to foster cross-border collaboration in healthcare research.

This section provides an analytical comparison of GDPR and KVKK, identifying areas of convergence and divergence that impact TRUMPET's technical, procedural, and legal compliance efforts.

Both GDPR and KVKK share a commitment to safeguarding data privacy, emphasizing principles that prioritize individual rights and secure data management. Central to both frameworks are core values such as data minimization, purpose limitation, accountability, and data security. These principles align seamlessly with the design of TRUMPET's federated learning platform, which processes data locally, ensuring only model updates are shared instead of raw data. This privacy-by-design approach underscores the project's dedication to secure data handling while fostering innovation in healthcare research.

Under GDPR, data subjects are afforded a broad set of rights designed to empower individuals and ensure transparency, as outlined in Articles 12–23. These include the right to access (Article 15), rectification (Article 16), erasure or the "right to be forgotten" (Article 17), restriction of processing (Article 18), data portability (Article 20), objection to processing (Article 21), and rights related to automated decision-making and profiling (Article 22). GDPR also emphasizes the right to receive clear and accessible information about data processing (Article 12).

Similarly, Türkiye's KVKK grants data subjects a range of rights under Article 11, reflecting comparable protections while incorporating certain nuances specific to Türkiye's legal framework. These rights include:

- **Right to Be Informed:** Data subjects must be informed about the identity of the data controller, the purpose of data processing, and to whom data may be transferred.
- **Right to Access Personal Data:** Individuals can request whether their data is processed and, if so, access their personal data.
- **Right to Rectification:** Data subjects can request the correction of incomplete or inaccurate data.
- **Right to Erasure:** Similar to GDPR's "right to be forgotten," individuals can request the deletion of personal data under certain conditions.

- Right to Restriction of Processing: Subjects can limit how their data is processed when accuracy or legitimacy is disputed.
- Right to Object: Individuals can object to the processing of their personal data for specific purposes, such as direct marketing.
- Right to Compensation: Data subjects can seek compensation for damages resulting from unlawful data processing.

One key difference lies in the specific mechanisms for data access and rectification. While GDPR provides a unified framework across the EU, KVKK emphasizes localized processes involving the Personal Data Protection Board (KVKK Board), which oversees compliance and resolves disputes.

By aligning with these rights, TRUMPET ensures its platform remains both GDPR and KVKK-compliant, offering robust data protection while maintaining the operational flexibility required for healthcare research.

On the other hand, despite these shared objectives, significant differences exist between GDPR and KVKK, influencing how TRUMPET must navigate regulatory compliance. The scope and territorial applicability of each framework is one area of divergence. GDPR extends its reach extraterritorially, applying to any organization processing the personal data of EU residents, irrespective of the organization's location. This global applicability requires TRUMPET to ensure that its operations involving EU users comply with GDPR's rigorous standards. In contrast, KVKK's jurisdiction is more localized, focusing primarily on Turkish entities or data concerning Turkish citizens. While it lacks GDPR's extraterritorial provisions, KVKK imposes stringent conditions on how data is handled and stored locally. Consequently, TRUMPET must adopt a dual compliance approach, aligning with GDPR's broad scope for EU users while meeting KVKK's specific requirements for Türkiye-based operations.

Despite shared objectives, GDPR and KVKK differ significantly in scope and territorial applicability, impacting TRUMPET's regulatory compliance strategy. GDPR's extraterritorial scope, as outlined in Article 3(2), applies to organizations outside the EU in two specific cases: when they process personal data of EU residents either by offering goods or services to them (whether for payment or not) or by monitoring their behaviour within the EU. This broad reach necessitates that TRUMPET ensures compliance with GDPR's stringent standards for any operations involving EU residents. In contrast, KVKK's jurisdiction focuses primarily on Türkiye-based entities or data concerning Turkish citizens, lacking GDPR's extraterritorial provisions. However, KVKK imposes strict rules on data storage and processing within Türkiye, requiring a tailored compliance approach. Consequently, TRUMPET must address these dual regulatory frameworks by adhering to GDPR's expansive scope for EU users while simultaneously meeting KVKK's detailed requirements for local operations.

Consent mechanisms also highlight notable differences. GDPR mandates explicit, informed, and unambiguous consent, particularly in contexts involving sensitive data like healthcare. It places a strong emphasis on the ability to withdraw consent as easily as it was given and transparency regarding data usage. KVKK, while similarly emphasizing the importance of clear consent, often demands even more detailed disclosures about the intended purposes and scope of data

processing. KVKK, while similarly emphasizing the importance of clear consent, often demands more detailed disclosures about the intended purposes and scope of data processing. For instance, under KVKK, organizations must specify not only the purpose of data collection but also outline in detail the legal grounds for processing, the potential transfer of data to third parties (including their identity and location), and the methods used for data collection. For example, if healthcare data is being collected, KVKK requires an explicit breakdown of whether the data will be used solely for medical diagnostics, shared with research institutions, or transferred abroad for analytics, each with specific permissions. These detailed requirements underscore the need for TRUMPET to develop a consent mechanism that aligns with KVKK's precise disclosure mandates while maintaining compliance with GDPR's broader transparency principles.

To reconcile these requirements, TRUMPET must incorporate a consent framework capable of balancing GDPR's demand for broad transparency with KVKK's need for specificity, ensuring that sensitive healthcare data is managed ethically and legally.

Cross-border data transfers present another critical challenge for TRUMPET. GDPR imposes strict conditions, requiring adequacy decisions or safeguards like Standard Contractual Clauses (SCCs) to ensure data protection during transfers. Similarly, KVKK restricts cross-border data flows but introduces specific criteria. Transfers are permitted to countries deemed to provide adequate protection; however, unlike the EU's adequacy decision procedure under GDPR, Türkiye's approach relies on assessments conducted by the Personal Data Protection Board (KVKK Board). Public details of these assessments or agreements are generally limited, creating uncertainties for organizations operating under KVKK.

TRUMPET's federated learning architecture inherently minimizes the risks associated with such transfers by processing data locally. Nonetheless, additional safeguards must be implemented under KVKK, such as obtaining explicit consent for cross-border transfers, ensuring comprehensive data processing agreements with clear clauses on security measures, and providing transparency to data subjects about the destination, purpose, and legal basis of the transfer. These measures ensure compliance with KVKK while aligning with GDPR's stringent standards.

Data breach notifications further illustrate the differences between the two frameworks. GDPR requires organizations to notify supervisory authorities and affected individuals within 72 hours of discovering a breach. KVKK, on the other hand, mandates timely notifications but allows for more procedural flexibility. For TRUMPET, this necessitates the development of a comprehensive incident response plan capable of adhering to GDPR's strict timelines while accommodating KVKK's procedural nuances. Data breach notifications highlight key differences between the General Data Protection Regulation (GDPR) and the Turkish Data Protection Law (KVKK). Under GDPR, organizations are required to notify supervisory authorities and affected individuals within 72 hours of becoming aware of a breach. This strict timeline ensures that personal data breaches are reported promptly, reducing the risk to data subjects.

On the other hand, KVKK mandates timely notification of data breaches but provides more procedural flexibility. Organizations must notify the Personal Data Protection Authority (KVKK) and affected individuals without undue delay. However, unlike GDPR, KVKK allows for adjustments in how notifications are managed. This flexibility enables organizations to tailor their approach to breach notifications based on specific circumstances, such as the scale or severity of the breach.

For TRUMPET, this necessitates the creation of a comprehensive incident response plan that balances GDPR's stringent 72-hour requirement with KVKK's procedural flexibility. Such a plan must ensure compliance with both frameworks by establishing clear processes for detecting, reporting, and managing data breaches. It should also incorporate collaboration between legal, compliance, and IT teams to effectively handle breaches while minimizing risks and ensuring data subject rights are upheld.

Overall, TRUMPET's incident response strategy must be robust enough to meet GDPR's strict deadlines while allowing for procedural adjustments as required by KVKK's nuanced approach to data breach notifications.

Integrating TRUMPET within this dual regulatory environment involves a strategic approach that harmonizes local and international legal requirements. Success hinges on a robust compliance framework that incorporates jurisdiction-specific adaptations, ensuring the platform operates seamlessly across regions. The federated learning model, with its inherent privacy-preserving features, provides a significant advantage, aligning with the privacy principles of both frameworks while supporting scalable and secure healthcare research.

Additionally, flexible consent management is crucial. The divergence in consent requirements between GDPR and KVKK necessitates a modular design for managing user consent, ensuring transparency and specificity across all jurisdictions. For instance, the KVKK places a stronger emphasis on obtaining explicit consent for the processing of sensitive personal data, such as health data, compared to GDPR, which allows for broader conditions under which consent can be obtained. Furthermore, the KVKK outlines stricter provisions regarding cross-border data transfers, limiting the scenarios under which personal data can be transferred abroad, whereas GDPR provides a more flexible framework. This necessitates a detailed understanding of both frameworks to ensure compliance. Moreover, mitigating risks associated with cross-border data transfers requires TRUMPET to prioritize localized data processing wherever possible while leveraging advanced privacy-preserving techniques. On the other hand, as the TRUMPET platform will not be used by the patients, there will be no need for patient consent management features.

Ultimately, the comparative analysis of GDPR and KVKK underscores the complexities of implementing TRUMPET across diverse regulatory landscapes. While both frameworks share a foundational commitment to data privacy and protection, their unique stipulations demand a tailored approach to compliance. By leveraging federated learning, strengthening consent mechanisms, and adopting robust governance practices, TRUMPET can successfully navigate these challenges. This balanced focus on privacy and innovation positions the project as a pioneering model for cross-border digital health initiatives, demonstrating the potential for technology to bridge regulatory divides while advancing healthcare research.

At this point table has been included at the end of this section to provide a clear overview of the articles in both regulatory frameworks where differences exist, along with how the "bridge" of compliance described in the section will be established.

Table 1: Regulatory Frameworks Comparison Table

Aspect	Relevant Article in EU GDPR	Relevant Article in KVKK	Difference/Gap	Proposed Compliance Bridge
Data Subject Rights	Article 15 (Right of Access)	Article 11 (Data Subject's Rights)	GDPR defines data subjects' rights in greater detail, while KVKK provides a more general approach.	Develop detailed implementation guidelines for KVKK to match GDPR standards.
Data Breach Notification	Article 33 (Notification)	Article 12(5)	GDPR imposes a 72-hour timeframe for breach notifications, which is not specified under KVKK.	Introduce a specific notification timeframe under KVKK, aligned with GDPR.
Data Transfer Provisions	Articles 44-50 (International Transfers)	Article 9	GDPR specifies mechanisms like SCCs (Standard Contractual Clauses), whereas KVKK lacks these.	Add SCC-equivalent mechanisms or establish agreements for data transfers under KVKK.
Consent Requirements	Article 7 (Conditions for Consent)	Article 5 (Explicit Consent)	GDPR includes more explicit provisions for withdrawal of consent; KVKK is less detailed on this.	Implement digital tools to simplify consent management under KVKK.
Data Protection Officer (DPO)	Articles 37-39 (Designation, Role)	No direct equivalent	GDPR mandates the appointment of a DPO; KVKK does not have such a requirement.	Introduce optional or incentivized guidelines for appointing a DPO-like role under KVKK.

3. Regulatory Challenges in Bridging GDPR and KVKK

The implementation of TRUMPET in Türkiye requires a nuanced approach to navigating the complexities of these dual frameworks. GDPR, which governs data protection within the EU, mandates high standards of transparency, explicit consent mechanisms, and stringent rules on data processing and cross-border transfers. In contrast, KVKK, while aligned with similar objectives, includes specific clauses tailored to Türkiye's unique regulatory and cultural context. These include provisions for data localization, the clarity of consent collection processes, and more flexible guidelines for data transfers under certain conditions.

First of all, GDPR places a strong emphasis on transparency, requiring organizations to provide clear, easily accessible information about how personal data will be used. It also mandates that explicit consent be obtained for data processing activities, ensuring that individuals fully understand and agree to how their data is handled. KVKK similarly requires transparency and consent but includes additional nuances specific to Türkiye's legal and cultural context. In Türkiye, the clarity of consent collection is given special importance, and organizations must ensure that consent is informed and freely given. Sensitive data categories, such as health or financial information, may require more stringent consent processes under KVKK.

Secondly, GDPR sets strict rules for data processing, giving individuals rights to access, rectify, and delete their personal data. Cross-border data transfers are highly regulated, requiring mechanisms like Standard Contractual Clauses or Binding Corporate Rules to ensure data protection when data is transferred outside the EU. In contrast, KVKK follows similar principles but provides more flexibility. While data localization is a significant feature, requiring certain types of sensitive data to be stored within Türkiye's borders, cross-border transfers are still possible under specific conditions. These transfers often require formal approval from Türkiye's Personal Data Protection Authority (KVKK), ensuring adequate safeguards are maintained.

Thirdly, KVKK mandates data localization for sensitive data such as health or financial information, meaning these data types must be stored within Türkiye's borders. This adds an additional layer of complexity compared to GDPR, which allows for international transfers with sufficient protection mechanisms. On the other hand, GDPR does not impose data localization requirements, providing organizations with more freedom to store and process data across different jurisdictions, provided that appropriate data protection measures are in place.

KVKK offers greater procedural flexibility, particularly in data transfer agreements. Organizations can adapt their approaches based on specific business needs and regulatory interpretations. In contrast, GDPR focuses on uniformity and strict compliance, ensuring consistent application of data protection rights across the EU without much room for flexibility.

For TRUMPET, navigating these dual frameworks involves understanding and managing these differences. The implementation must address GDPR's rigid timelines and standards while also accommodating the more flexible, contextual guidelines of KVKK. Ensuring compliance with both

frameworks requires balancing transparency, consent processes, data localization, and handling cross-border transfers effectively.

One of the critical areas of focus for TRUMPET is cross-border data transfers. Under GDPR, data transfers to non-EU countries are subject to strict conditions, requiring either an adequacy decision or robust contractual safeguards such as Standard Contractual Clauses (SCCs). KVKK, similarly, restricts data transfers outside Türkiye but offers additional flexibility, such as recognizing countries deemed to provide adequate protection or allowing transfers under specific agreements. For a project like TRUMPET, which seeks to foster cross-border collaboration, these differences necessitate the development of tailored data governance strategies that satisfy both GDPR's strict requirements and KVKK's locally adapted provisions. This means implementing a dual compliance system that ensures data can be shared effectively without compromising the privacy rights of individuals in either jurisdiction. Such strategies may include maintaining separate data environments for EU and Turkish users or employing advanced encryption and pseudonymization techniques to facilitate secure data flows.

Additionally, consent mechanisms under the two frameworks present another layer of complexity. GDPR emphasizes the need for explicit, informed, and freely given consent, particularly when processing sensitive data such as health information. KVKK, while similarly stringent, requires detailed clarity in how consent is obtained and processed, often demanding more specific disclosures about data usage. This necessitates TRUMPET's platform to adopt a dynamic and customizable consent framework capable of meeting the granular requirements of both GDPR and KVKK. For example, the platform must provide users with clear, easily understandable consent forms tailored to the context of each jurisdiction, along with accessible options for consent withdrawal. This not only ensures legal compliance but also enhances user trust and participation in the platform.

Therefore, the TRUMPET project has undertaken a comprehensive strategy to bridge the regulatory frameworks of GDPR and KVKK. This involves a meticulous analysis of both frameworks, identifying areas of convergence and divergence, and integrating these insights into the platform's technical and procedural design. By leveraging federated learning's inherent privacy-preserving capabilities, TRUMPET not only addresses compliance challenges but also positions itself as a model for innovation in secure healthcare research. This dual approach ensures that the project not only adheres to the highest standards of data protection but also fosters collaboration and trust across borders.

4. Integration Process for the TRUMPET Platform in Türkiye as a Non-EU Country

The integration of the TRUMPET platform into Türkiye's healthcare system involves addressing a range of technical and procedural challenges. These challenges arise from the need to comply with both the European General Data Protection Regulation (GDPR) and Türkiye's Personal Data Protection Law (KVKK), while maintaining the platform's federated learning capabilities to support advanced healthcare data analytics and research initiatives.

To achieve seamless integration, several technical modifications and rigorous validation processes are required to ensure adherence to local and international regulatory frameworks.

4.1. Technical Modifications for Local Compliance

Adapting the TRUMPET platform to Türkiye's unique regulatory and technical environment requires specific updates to its architecture and processes.

One of the foremost challenges in integrating the TRUMPET platform lies in adapting its federated learning models to Türkiye's specific regulatory context. Federated learning, which allows collaborative data analysis without transferring raw data, must be configured to ensure compliance with KVKK's principles of data protection. This requires implementing advanced encryption protocols to safeguard sensitive information during model training. Furthermore, data anonymization techniques are employed to strip personal identifiers from datasets, ensuring patient privacy remains uncompromised.

These principles are essential when compared to GDPR, which similarly emphasizes strong data protection standards. GDPR mandates transparency, data minimization, and the implementation of appropriate safeguards, such as pseudonymization and encryption, to protect personal data. Both frameworks highlight the importance of protecting sensitive information, yet GDPR places a greater emphasis on rights such as access, rectification, and the right to be forgotten, whereas KVKK focuses on specific, contextual requirements tailored to Türkiye's legal framework.

Additionally, mechanisms to limit cross-border data transfers have been incorporated. In Türkiye's regulatory environment, the movement of healthcare data beyond national borders is subject to stringent controls such as data localization requirements, formal approval from the Personal Data Protection Authority (KVKK), Standard Contractual Clauses (SCCs), strict data minimization and anonymization. Regarding the data localization requirements, certain types of sensitive healthcare data, such as health and financial information, must be stored within Türkiye's borders. This ensures that personal data is not transferred internationally without adequate safeguards. Regarding the formal approval from KVKK, any cross-border data transfer involving healthcare data must receive explicit approval from Türkiye's Personal Data Protection Authority (KVKK). This ensures that data processing practices align with Türkiye's legal standards. Regarding the SCCs, while KVKK provides flexibility in certain cases, cross-border transfers may require tailored contractual agreements, such as SCCs, to safeguard data during international transfers. And lastly, regarding the strict data minimization and anonymization, ensuring that only necessary data is processed and employing techniques like anonymization to prevent the identification of individuals, especially in sensitive healthcare contexts. The platform has been modified to enforce these restrictions, ensuring all data

processing and storage activities occur within Türkiye's jurisdiction. This not only mitigates legal risks but also strengthens trust among stakeholders, particularly patients and healthcare institutions.

4.2. Testing and Validation

To ensure the platform's operational and regulatory readiness, a comprehensive testing and validation process has been established. This process is integral to verifying the platform's secure operation within the Ministry of Health's (MOH) infrastructure and its alignment with local regulations.

The first stage involves integration testing, which focuses on the technical compatibility of the TRUMPET platform with the MOH's existing systems. These tests evaluate the effectiveness of encryption protocols, the functionality of data export restrictions, and the overall adherence to local data processing and storage standards.

Subsequent system testing assesses the platform's real-world performance within Türkiye's healthcare environment. This includes verifying the secure flow of healthcare data across interoperable systems, ensuring the platform's functionality aligns with the operational needs of healthcare providers. Emphasis is placed on maintaining the privacy and security of patient data during all exchanges.

Finally, compliance validation is conducted as the concluding step in the integration process. This phase involves a meticulous review of all data handling procedures, patient consent mechanisms, and safeguards implemented for secure data transfer. The validation process ensures that both GDPR and KVKK requirements are fully met, providing confidence in the platform's ability to maintain the confidentiality, integrity, and security of sensitive healthcare information throughout its lifecycle.

This structured approach to integration not only guarantees compliance but also enhances the overall functionality and reliability of the TRUMPET platform, enabling it to serve as a robust tool for advancing healthcare research and analytics in Türkiye.

4.3. Broader Implications for Türkiye's Healthcare System

The successful integration of the TRUMPET platform within Türkiye represents a significant advancement in the nation's healthcare infrastructure. By leveraging federated learning, the platform enables innovative healthcare research and analytics without compromising patient privacy. This approach not only aligns with Türkiye's commitment to modernizing its healthcare services but also positions the country as a leader in adopting cutting-edge, privacy-preserving technologies.

One of the critical implications of TRUMPET's implementation is its potential to bridge gaps in healthcare accessibility and equity. By fostering collaborations among healthcare institutions and research centers, the platform enables the development of predictive models and diagnostic tools that cater to diverse patient populations. This is particularly crucial in Türkiye, where regional disparities in healthcare access remain a challenge. The decentralized nature of federated learning ensures that institutions across the country, regardless of their technological maturity, can participate in and benefit from the platform's capabilities.

Furthermore, the integration of TRUMPET emphasizes the importance of adopting global best practices while addressing local needs. Türkiye's regulatory alignment efforts with GDPR and KVKK demonstrate its readiness to participate in international healthcare innovation ecosystems. This dual compliance not only facilitates cross-border research collaborations but also bolsters Türkiye's reputation as a reliable partner in global health initiatives. Such positioning is likely to attract more international projects and investments, further enhancing the country's healthcare R&D capacity.

In addition to its regulatory and technological contributions, TRUMPET is poised to impact public trust in digital health technologies. Privacy concerns are often a significant barrier to adopting advanced healthcare solutions. By demonstrating a robust commitment to data protection through federated learning and adherence to GDPR and KVKK standards, the platform reinforces public confidence in Türkiye's digital health ecosystem. As citizens see their data being handled securely and ethically, they are more likely to engage with digital health solutions, paving the way for broader acceptance of future innovations.

Lastly, the success of TRUMPET underscores the potential for Türkiye to serve as a testing ground for scalable healthcare technologies. The lessons learned from this project can inform the development of similar platforms tailored for other sectors, such as education or social services. By showcasing its ability to harmonize local and international standards, Türkiye can position itself as a leader in digital transformation and a model for other countries navigating similar challenges. TRUMPET, therefore, represents not just a milestone in healthcare but also a catalyst for broader advancements in Türkiye's technological and regulatory landscapes.

5. Conclusion

The integration of TRUMPET within Türkiye serves as a pivotal case study in demonstrating the adaptability and resilience required to ensure regulatory alignment for federated learning across both EU and non-EU borders. This deliverable provides essential insights into the customization of federated models in healthcare settings, ensuring that the application of these technologies is in full compliance with rigorous data privacy regulations, ethics, and local governance standards. By focusing on GDPR and KVKK (the Turkish Data Protection Law), it highlights how sensitive health data can be managed securely while facilitating cross-border collaboration.

These findings not only contribute to the refinement of federated learning models in healthcare but also offer actionable recommendations that can be adopted by similar projects in different jurisdictions. The adaptability demonstrated in the TRUMPET project lays the groundwork for expanding such models globally, supporting healthcare research while maintaining strict adherence to privacy laws and ethical principles.

Furthermore, this project illustrates the critical role of interdisciplinary collaboration in overcoming complex regulatory and technical challenges. By bringing together expertise in healthcare, data science, and legal compliance, TRUMPET has successfully navigated the intricacies of dual regulatory frameworks. This approach not only ensures the project's success but also provides a replicable blueprint for other countries and regions seeking to implement federated learning technologies in compliance with diverse regulatory environments.

The lessons learned from TRUMPET's integration into Türkiye's healthcare landscape also underscore the potential for federated learning to revolutionize data-driven healthcare research globally. By maintaining high standards of privacy and security, the project exemplifies how technological innovation can be harmonized with patient-centric values. This balance of innovation and compliance is essential for fostering trust among stakeholders, including patients, healthcare providers, and policymakers, ensuring the long-term viability and impact of such initiatives.

In conclusion, this integration underscores the critical importance of aligning technological advancements with both legal and ethical frameworks. It emphasizes how careful consideration of GDPR-KVKK compatibility can enhance data security and foster regulatory compliance, creating a digital health framework that is sustainable and ethically responsible. This initiative not only benefits Türkiye's healthcare landscape but also sets a significant precedent for similar federated learning projects across Europe and beyond. Through this integration, TRUMPET exemplifies the potential of federated learning to advance global healthcare research, paving the way for future innovations in the field while safeguarding patient rights and fostering international collaboration.

References

- European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). Official Journal of the European Union. Retrieved from <https://eur-lex.europa.eu>
- Türkiye. (2016). Kişisel Verilerin Korunması Kanunu (Law No. 6698 on the Protection of Personal Data – KVKK). Official Gazette of the Republic of Türkiye. Retrieved from <https://www.kvkk.gov.tr>